How Clean is Your Workspace?

Written by Randy Fisher, Department of Technology Services
Thursday, 16 July 2009 13:23 - Last Updated Thursday, 16 July 2009 13:38

The protection of information and equipment is a not only important for employees, it is often mandated by statute. Each of us should be doing our part to secure our workspaces, conference rooms and other common areas. Below are some guidelines to follow:

- **Clean Desk Policy:** Many of the security requirements can be met by simply keeping an orderly workspace. Desks, credenzas, and workstations should be cleared and locked at the end of each day. The close tie between cleanliness and security is necessary.
- **Confidential or other sensitive information:** Clear workstations or meeting rooms of all work materials (including confidential items) at the end of the workday or when they will be unattended for extended periods during the business day. Confidential materials include client data, passwords, network information, product development specs, financials, direct-line phone lists, and other materials you would not want to fall into the wrong hands.
- **Access to your files and the network:** You should always shut down your system before leaving. Turning off the monitor is not the same as shutting down the system. If you cannot shut down, use a password protected screensaver. If you have Windows 2000 or Windows XP, use the lock-out feature.
- **Laptop computers:** All laptop computers should be secured in a locked cabinet or locked with a cable, or taken with you when leaving.
- **Palm Pilot or other small electronic devices:** These items should be secured in a locked cabinet or taken with you when leaving. This includes all hand-held computers, removable hard drives, and other computer peripherals, cameras, test equipment, video equipment, cell phone and other valuables.
- **Security of drawers and cabinets:** Lock all drawers and cabinets, except pencil drawer. Use caution in leaving valuables in the pencil drawer.
- **Sensitive information in common areas:** Common areas should be secured. White boards, easel pads and computer screens displaying sensitive information should not be left unsecured or visible through outside windows.
- **Proper disposal of sensitive media:** Be mindful of how you dispose of sensitive media

How Clean is Your Workspace?

Written by Randy Fisher, Department of Technology Services
Thursday, 16 July 2009 13:23 - Last Updated Thursday, 16 July 2009 13:38

and information. Back-up media, whether on tapes, CDs or paper, should not go in an open trash can. Sensitive media should be destroyed or locked up.
Confidential recycle bins can be used to dispose of any confidential information printed on paper. Contact your data disposal technician for details on how to dispose of large quantities of media.

We appreciate your cooperation in helping maintain a secure work environment for our employees, customers and citizens!